Journal of Symbolic Computation 46 (2011) 1291–1305

Contents lists available at SciVerse ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

When does $\langle T \rangle$ equal sat(T)?☆

François Lemaire [b], Marc Moreno Maza [a,1], Wei Pan [a], Yuzhen Xie [a]

[a] *University of Western Ontario, Department of Computer Science, London, Ontario, Canada N6A 5B7*
[b] *University Lille 1, France*

ARTICLE INFO

Article history:
Received 6 January 2009
Accepted 30 July 2011
Available online 30 August 2011

Keywords:
Regular chain
Saturated ideal
Primitivity of polynomials

ABSTRACT

Given a regular chain T, we aim at finding an efficient way for computing a system of generators of sat(T), the saturated ideal of T. A natural idea is to test whether the equality $\langle T \rangle = \text{sat}(T)$ holds, that is, whether T generates its saturated ideal. By generalizing the notion of primitivity from univariate polynomials to regular chains, we establish a necessary and sufficient condition, together with a Gröbner basis free algorithm, for testing this equality. Our experimental results illustrate the efficiency of this approach in practice.

1. Introduction

Triangular decompositions are one of the most studied techniques for solving polynomial systems symbolically. Invented by J.F. Ritt in the early 30's for systems of differential polynomials, their stride started in the late 80's with the method of Wu (1986) dedicated to algebraic systems. Different concepts and algorithms extended the work of Wu. In the early 90's, the notion of a *regular chain*, introduced independently by Kalkbrener (1993) and by Yang and Zhang (1991), led to important algorithmic discoveries.

In Kalkbrener's vision, regular chains are used to represent the generic zeros of the irreducible components of an algebraic variety. In the original work of Yang and Zhang, they are used to decide whether a hypersurface intersects a quasi-variety (given by a regular chain). Regular chains have, in fact, several interesting properties and are the key notion in many algorithms for decomposing systems of algebraic or differential equations.

☆ This research was partly supported by NSERC, Maplesoft and MITACS of Canada.
E-mail addresses: Francois.Lemaire@lifl.fr (F. Lemaire), moreno@csd.uwo.ca (M. Moreno Maza), wpan9@csd.uwo.ca (W. Pan), yxie@csail.mit.edu (Y. Xie).
[1] Tel.: +1 519 878 04 06; fax: +1 519 661 35 65.

0747-7171/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2011.08.010

Regular chains have been investigated in many papers, among them are those of Aubry et al. (1999), Kalkbrener (1998) and Chou and Gao (1991). Several surveys (Boulier et al., 2006; Hubert, 2001) are also available on this topic. The abundant literature on the subject can be explained by the many equivalent definitions of a regular chain. Actually, the original formulation of Kalkbrener is quite different from that of Yang and Zhang. In the papers by Chen et al. (2007) and Wang (2000), the authors provide bridges between the point of view of Kalkbrener and that of Yang and Zhang.

The key algebraic object associated with a regular chain is its *saturated ideal*. Let us review its definition. Let $\mathbf{k}$ be a field and $x_1 \prec \cdots \prec x_n$ be ordered variables. For a regular chain $T \subset \mathbf{k}[x_1, \ldots, x_n]$, the saturated ideal of T, denoted by $\mathrm{sat}(T)$ is defined by $\mathrm{sat}(T) := \langle T \rangle : h^\infty$, where h is the product of the initial polynomials of T. (The next section contains a detailed review of these notions.) Given a polynomial $p \in \mathbf{k}[x_1, \ldots, x_n]$, the memberships $p \in \mathrm{sat}(T)$ and $p \in \sqrt{\mathrm{sat}(T)}$ can be decided by means of pseudo-divisions and GCD computations, respectively. One should observe that these computations can be achieved without computing a system of generators of $\mathrm{sat}(T)$. In some sense, the regular chain T is a "black box representation" of $\mathrm{sat}(T)$ since the assertions $p \in \mathrm{sat}(T)$ and $p \in \sqrt{\mathrm{sat}(T)}$ can be evaluated without using an explicit representation of $\mathrm{sat}(T)$.

Being able to compute a system of generators of $\mathrm{sat}(T)$ remains, however, a fundamental question. For instance, given a second regular chain $U \subset \mathbf{k}[x_1, \ldots, x_n]$, the only general method to decide the inclusion $\mathrm{sat}(T) \subseteq \mathrm{sat}(U)$ goes through the computation of a system of generators of $\mathrm{sat}(T)$ by means of Gröbner bases. Unfortunately, such computations can be expensive (see Aubry and Moreno Maza, 1999) whereas one would like to obtain an inclusion test which could be used intensively in order to remove redundant components when computing the triangular decompositions of Kalkbrener's algorithm or those arising in differential algebra. Note that for other kinds of triangular decompositions, such as those of Moreno Maza (1999) and Wang (2000), this question has been solved in Chen et al. (2007).

Therefore, testing the inclusion $\mathrm{sat}(T) \subseteq \mathrm{sat}(U)$ without Gröbner basis computation is a very important question in practice. Moreover, this can be regarded as an *algebraic version* of the Ritt problem in differential algebra. One case presents no difficulties: if $\mathrm{sat}(T)$ is a zero-dimensional ideal, the product of the initial polynomials of T is invertible modulo $\langle T \rangle$ (see Moreno Maza and Rioboo, 1995, Proposition 5) and thus T generates $\mathrm{sat}(T)$. In this case, the inclusion test for saturated ideals reduces to the membership problem mentioned above.

In positive dimension, however, the ideal $\mathrm{sat}(T)$ could be strictly larger than that generated by T. Consider for instance $n = 4$ and $T = \{x_1x_3 + x_2, x_2x_4 + x_1\}$, we have

$$\langle T \rangle = \langle x_1, x_2 \rangle \cap \langle x_1x_3 + x_2, -x_3x_4 + 1 \rangle.$$

Thus, we have

$$\mathrm{sat}(T) = \langle T \rangle : (x_1x_2)^\infty = \langle x_1x_3 + x_2, -x_3x_4 + 1 \rangle.$$

In this article, we give a necessary and sufficient condition for the equality $\langle T \rangle = \mathrm{sat}(T)$ to hold. Looking at the above example, one can feel that the ideal $\langle x_1, x_2 \rangle$ can be regarded as a "sort of content" of the ideal $\langle T \rangle$, which is discarded when computing $\mathrm{sat}(T)$. We observe also that the polynomials $x_1x_3 + x_2$ and $x_2x_4 + x_1$ are primitive in $(\mathbf{k}[x_1, x_2])[x_3]$ and $(\mathbf{k}[x_1, x_2])[x_4]$, respectively. Thus, the "usual notion" of primitivity (for a univariate polynomial over a UFD) is not sufficient to guarantee the equality $\langle T \rangle = \mathrm{sat}(T)$. This leads us to the following two definitions.

Let R be a commutative ring with unity. We say that a non-constant polynomial $p = a_e x^e + \cdots + a_0 \in R[x]$ is *weakly primitive* if for any $\beta \in R$ such that a_e divides $\beta a_{e-1}, \ldots, \beta a_0$ then a_e divides β as well. This notion and its relations with similar concepts are discussed in Sections 3–5.

We say that the regular chain $T = \{p_1, \ldots, p_m\}$ is *primitive* if for all $1 \leq k \leq m$, the polynomial p_k is weakly primitive in $R[x_j]$, where x_j is the main variable of p_k and R is the residue class ring $\mathbf{k}[x_1, \ldots, x_{j-1}]/\langle p_1, \ldots, p_{k-1} \rangle$.

The first main result of this paper is the following: *the regular chain T generates its saturated ideal if and only if T is primitive.* This result, generalizing the concept of primitivity from univariate polynomials to regular chains, is established in Section 4.

Looking at regular chains from the point of view of regular sequences, we obtain our second main result: an algorithm to decide whether a regular chain generates its saturated ideal or not. The

pseudo-code and its proof are presented in Section 6. This algorithm relies on a procedure for computing triangular decompositions. However, being applied to input systems which are regular sequences and "almost regular chains", this procedure reduces simply to an iterated resultant computation. As a result, the proposed algorithm performs very well in practice and is Gröbner basis free. In Section 8, we report on experimentation, where we confirm the efficiency of this algorithm. Meanwhile, we observe that primitive regular chains are often present in the output of triangular decompositions.

Section 7, which is a new development w.r.t. our ISSAC paper (Lemaire et al., 2008), proposes several criteria for testing the inclusion of saturated ideals. We point out that the notion of primitivity of regular chains provides a helpful tool for dealing with this question in practice. Section 9, which is also enhanced w.r.t. (Lemaire et al., 2008), offers concluding remarks and open problems.

2. Preliminaries

This section reviews the basic notions related to regular chains. Then, with Theorems 1 and 2 below, we recall important results which will be used throughout this paper.

Commutative rings and ideals. Let R be a commutative ring with unity and F be a subset of R. Denote by $\langle F\rangle$ the *ideal* it generates, by $\sqrt{\langle F\rangle}$ the radical of $\langle F\rangle$, and by $R/\langle F\rangle$ the *residue class ring* of R with respect to $\langle F\rangle$. For an element p in R, we say that p is zero modulo $\langle F\rangle$ if p belongs to $\langle F\rangle$. An element $p \in R$ is a *zerodivisor* modulo $\langle F\rangle$, if there exists $q \in R$ such that $p \notin \langle F\rangle$ and $q \notin \langle F\rangle$ but $pq \in \langle F\rangle$. We say that p is *regular* modulo $\langle F\rangle$ if it is neither zero, nor a zerodivisor modulo $\langle F\rangle$. Furthermore, p is *invertible* in R if there exists a $q \in R$ such that $p\,q = 1$.

Multivariate polynomials. We denote by $\mathbf{k}[\boldsymbol{x}]$ the ring of multivariate polynomials with coefficients in a field $\mathbf{k}$ and with ordered variables $\boldsymbol{x} = x_1 \prec \cdots \prec x_n$. For a non-constant polynomial $p \in \mathbf{k}[\boldsymbol{x}]$, the greatest variable in p is called *main variable*, denoted by $\mathrm{mvar}(p)$. We regard p as a univariate polynomial in its main variable. The degree, the leading coefficient, the leading monomial and the reductum of p as a univariate polynomial in $\mathrm{mvar}(p)$ are called *main degree, initial, rank* and *tail* of p; they are denoted by $\mathrm{mdeg}(p)$, $\mathrm{init}(p)$, $\mathrm{rank}(p)$ and $\mathrm{tail}(p)$, respectively. Thus, we have $p = \mathrm{init}(p)\mathrm{rank}(p) + \mathrm{tail}(p)$. We say that an ideal of $\mathbf{k}[\boldsymbol{x}]$ is *unmixed*, if all its associated primes have the same dimension.

Triangular set and regular chain. A set T of non-constant polynomials in $\mathbf{k}[\boldsymbol{x}]$ is called a *triangular set*, if for all $p, q \in T$ with $p \neq q$ we have $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$. For a nonempty triangular set T, we define the *saturated ideal* $\mathrm{sat}(T)$ of T to be the ideal $\langle T\rangle : h^\infty$, that is, $\mathrm{sat}(T) := \{q \in \mathbf{k}[\boldsymbol{x}] \mid \exists e \in \mathbb{Z}_{\geq 0} \text{ s.t. } h^e q \in \langle T\rangle\}$, where h is the product of the initials of the polynomials in T. The empty set is also regarded as a triangular set, whose saturated ideal is the trivial ideal $\langle 0\rangle$. Let T be a triangular set in $\mathbf{k}[\boldsymbol{x}]$. If T is empty, then it is a regular chain. Otherwise, let p be the polynomial of T with the greatest main variable and let T' be the set of other polynomials in T: we say that T is a *regular chain*, if T' is a regular chain and $\mathrm{init}(p)$ is regular modulo $\mathrm{sat}(T')$.

Regular chain and regular sequence. In commutative algebra (see Eisenbud, 1994) there is a concept called *regular sequence*, closely related to that of a regular chain. This is a sequence $r_1, \ldots, r_s$ of nonzero elements in the ring $\mathbf{k}[\boldsymbol{x}]$ satisfying

(1) $\langle r_1, \ldots, r_s\rangle$ is a proper ideal of $\mathbf{k}[\boldsymbol{x}]$;
(2) r_i is regular modulo $\langle r_1, \ldots, r_{i-1}\rangle$, for each $2 \leq i \leq s$.

When we sort polynomials in a regular chain by increasing main variable, the following example says that the resulting sequence may not be a regular sequence of $\mathbf{k}[\boldsymbol{x}]$. Consider for instance the regular chain $T = \{t_1, t_2\} \subset \mathbf{k}[x_1, x_2, x_3]$ with $t_1 = x_1x_2$ and $t_2 = x_1x_3$. Observe that t_1, t_2 is not a regular sequence since t_2 is not regular modulo $\langle t_1\rangle$.

The pseudo-division formula. Let p and q be polynomials of $\mathbf{k}[\boldsymbol{x}]$, with $q \notin \mathbf{k}$. Denote by $\mathrm{prem}(p, q)$ and $\mathrm{pquo}(p, q)$ the *pseudo-remainder* and the *pseudo-quotient* of p by q, regarding p and q as univariate polynomials in $x = \mathrm{mvar}(q)$. Using these notations, we have $\mathrm{init}(q)^e p = \mathrm{pquo}(p, q)q + \mathrm{prem}(p, q)$, where $e = \max\{\deg(p, x) - \deg(q, x) + 1, 0\}$; moreover either $r := \mathrm{prem}(p, q)$ is null or $\deg(r, x) < \deg(q, x)$. Given a polynomial p and a regular chain T, pseudo-division generalizes as follows. If $T = \emptyset$, we define $\mathrm{prem}(p, T) = p$. Otherwise, letting t be the polynomial in T with the greatest main variable,

we define $\mathrm{prem}(p, T) = \mathrm{prem}(\mathrm{prem}(p, t), T')$, with $T = T' \cup \{t\}$. We have the *pseudo-division formula* (Wu, 1986): there exist non-negative integers $e_1, \ldots, e_s$ and polynomials $q_1, \ldots, q_s$ in $\mathbf{k}[\boldsymbol{x}]$ such that $h_1^{e_1} \cdots h_s^{e_s} p = \sum_{i=1}^{s} q_i t_i + \mathrm{prem}(p, T)$, where $T = \{t_1, \ldots, t_s\}$ and $h_i = \mathrm{init}(t_i)$, for $1 \leq i \leq s$.

Iterated resultant. We denote by $\mathrm{res}(p, q)$ the *resultant* of p and q regarding them as univariate polynomials in $\mathrm{mvar}(q)$. Note that $\mathrm{res}(p, q)$ may be different from $\mathrm{res}(q, p)$, if they have different main variables. For a polynomial p and a regular chain T, we define the *iterated resultant* of p w.r.t. T, denoted by $\mathrm{ires}(p, T)$, as follows. If $T = \emptyset$, then we define $\mathrm{ires}(p, T) = p$. Otherwise, letting t be the polynomial in T with the greatest main variable, we define $\mathrm{ires}(p, T) = \mathrm{ires}(\mathrm{res}(p, t), T')$, with $T = T' \cup \{t\}$.

Theorem 1. *For a regular chain T and a polynomial p we have:*

(1) *p is zero modulo $\mathrm{sat}(T)$ if and only if $\mathrm{prem}(p, T) = 0$,*
(2) *p is regular modulo $\mathrm{sat}(T)$ if and only if $\mathrm{ires}(p, T) \neq 0$,*
(3) *p is a zerodivisor modulo $\mathrm{sat}(T)$ if and only if $\mathrm{ires}(p, T) = 0$ and $\mathrm{prem}(p, T) \neq 0$.*

For the proofs, we refer to Aubry et al. (1999) for item (1), and to Wang (2000); Chen et al. (2007) for item (2). Item (3) is a direct consequence of (1) and (2).

Theorem 2. *Let $T = T' \cup \{t\}$ be a regular chain in $\mathbf{k}[\boldsymbol{x}]$ with t having the greatest main variable in T. The following properties hold:*

(1) *$\mathrm{sat}(T)$ is an unmixed ideal with dimension $n - |T|$,*
(2) *$\mathrm{sat}(T \cap \mathbf{k}[x_1, \ldots, x_i]) = \mathrm{sat}(T) \cap \mathbf{k}[x_1, \ldots, x_i]$, for all $i = 1 \cdots n$,*
(3) *$\mathrm{sat}(T) = \langle \mathrm{sat}(T') \cup \{t\} \rangle : \mathrm{init}(t)^{\infty}$.*

For the proofs, we refer to Boulier et al. (2006); Chou and Gao (1991) for item (1), to Aubry et al. (1999) for item (2), and to Kalkbrener (1998) for item (3). From (1), we deduce that the saturated ideal of a regular chain T consisting of n polynomials has dimension 0. Theorems 1 and 2 highlight the structure of the associated primes of $\mathrm{sat}(T)$ which makes the regularity test easier than with an arbitrary polynomial ideal. In general, deciding if a polynomial p is regular modulo an ideal $\mathcal{I}$ of $\mathbf{k}[\boldsymbol{x}]$ is equivalent to checking if p does not belong to any associated primes of I.

3. Primitivity of polynomials

We introduce the notion of weak primitivity of a polynomial in a general univariate polynomial ring, and present several of its properties. The following Lemma 1 may be seen as a generalization of Gauss Lemma over an arbitrary commutative ring. It will be used in the proof of our main theorem. We found that this lemma can be deduced from the Dedekind–Mertens Lemma (see Arnold and Gilmer (1970); Corso et al. (1998); Coquand et al. (2003) and the references therein). For the sake of reference, we include a direct proof. In the sequel, the ring R is a commutative Noetherian ring with unity. We say that $p \in R$ divides $q \in R$ and write $p \mid q$, if there exists $r \in R$ such that $q = p\,r$ holds.

Lemma 1. *Let $p = \sum_{i=0}^{m} a_i y^i$ and $q = \sum_{i=0}^{n} b_i y^i$ be polynomials in $R[y]$ with $\deg(p) = m \geq 0$ and $\deg(q) = n \geq 0$. Then for each $h \in R$,*

(i) *$h \mid pq$ implies $h \mid b_0 a_i^{n+1}$ for $0 \leq i \leq m$,*
(ii) *$h \mid pq$ implies $h \mid b_n a_i^{n+1}$ for $0 \leq i \leq m$.*

Proof. First, we prove (i). Considering first the special case $m = 0$, we observe that $h \mid pq$ implies $h \mid a_0 b_0$ and the conclusion follows. Now we assume that $m > 0$ holds.

For $i = 0$, the claim is also clear, for the same reason as the case $m = 0$. For $1 \leq i \leq m$, we introduce the polynomials A_i and B_i below in order to simplify our expressions:

$$A_i = \sum_{j=0}^{i-1} a_j y^j, \quad \text{and} \quad B_i = -\sum_{j=i}^{m} a_j y^j. \tag{1}$$

Clearly, we have $p = A_i - B_i$. The key observation is to consider the polynomial $\tilde{p} = A_i^{n+1} - B_i^{n+1}$, as suggested by the forms of our claims. To avoid talking about the degree of a zero polynomial, we

assume that both A_i^{n+1} and B_i^{n+1} are nonzero polynomials. From (1), we have the following degree estimates:

$$\deg(A_i^{n+1}) \le \deg(A_i)(n+1) \le (i-1)(n+1), \tag{2}$$

$$\operatorname{trdeg}(B_i^{n+1}) \ge \operatorname{trdeg}(B_i)(n+1) \ge i(n+1), \tag{3}$$

where $\operatorname{trdeg}(\cdot)$ denotes the trailing degree, that is, the degree of the term with lowest degree in a polynomial. Therefore there is no term cancelation between A_i^{n+1} and B_i^{n+1}. Since A_i and B_i are nonzero, the polynomial $\tilde{p}$ is nonzero too. Moreover, $\tilde{p}$ factorizes as

$$\tilde{p} = (A_i - B_i)(A_i^n + \cdots + B_i^n) = p(A_i^n + \cdots + B_i^n).$$

It follows that $p \mid \tilde{p}$ holds. Therefore $h \mid \tilde{p}q$ holds since we have $h \mid pq$. Observe now that if qA_i^{n+1} is nonzero, then we have

$$\deg(qA_i^{n+1}) \le (i-1)(n+1) + n < i(n+1). \tag{4}$$

Similarly, if qB_i^{n+1} is nonzero, then its trailing degree satisfies $\operatorname{trdeg}(qB_i^{n+1}) \ge i(n+1)$. Combining with (4), we deduce that in $q\tilde{p} = qA_i^{n+1} - qB_i^{n+1}$, the polynomial qA^{n+1} only contributes to terms with degree smaller than $i(n+1)$. Thus we have

$$\operatorname{coeff}(q\tilde{p}, y^{i(n+1)}) = \operatorname{coeff}(-qB_i^{n+1}, y^{i(n+1)}) = b_0 a_i^{n+1} \tag{5}$$

which implies $h \mid b_0 a_i^{n+1}$, as desired. Now we handle the special cases, where $A_i^{n+1} = 0$ and $B_i^{n+1} = 0$. It is easy to see that $A_i^{n+1} = 0$ does not affect the proof above. When $B_i^{n+1} = 0$, simply we have $a_i^{n+1} = 0$, and then the claim is also clear.

Finally, we prove (ii). Let $P = y^m p(1/y)$ and $Q = y^n q(1/y)$. Since $h \mid pq$, h will also divide $PQ = y^{m+n}(pq)(1/y)$. Assume that $a_0 = \cdots = a_{r-1} = 0$, $a_r \ne 0$ and $b_0 = \cdots = b_{s-1} = 0$, $b_s \ne 0$ hold. Then $r \le m$ and $s \le n$ hold. According to (i), for any $r \le i \le m$, $h \mid b_n a_i^{s+1}$. It follows that $h \mid b_n a_i^{n+1}$ for any $0 \le i \le m$. □

Definition 1. Let $p = a_0 + \cdots + a_e x^e \in R[x]$ with $e \ge 1$. The polynomial p is *strongly primitive* if the ideal generated by $a_0, \ldots, a_e$ is R. The polynomial p is *weakly primitive* if for any $\beta \in R$ such that $a_e \mid \beta a_i$ holds for all $0 \le i \le e-1$, we have $a_e \mid \beta$ as well.

Proposition 1. *Strong primitivity implies weak primitivity.*

Proof. We use the same notation as in Definition 1. Let p be strongly primitive. Then there exist $c_e, \ldots, c_0 \in R$ such that $c_e a_e + \cdots + c_0 a_0 = 1$. Let $\beta \in R$ such that for $0 \le j \le e-1$, we have $a_e \mid \beta a_j$. Then there exist $d_0, \ldots, d_{e-1} \in R$ such that $a_e d_j = \beta a_j$. Since $\beta c_e a_e + \cdots + \beta c_0 a_0 = \beta$, we have $a_e(\beta c_e + d_{e-1}c_{e-1} \cdots + d_0 c_0) = \beta$. Thus, we have $a_e \mid \beta$, and therefore p is weakly primitive. □

Remark 1. With the above notation, we first observe that, if one coefficient is invertible, then p is strongly primitive and thus it is also weakly primitive. Next, we observe that weak primitivity does not imply strong primitivity. For example, let $R = \mathbb{Z}[t]$ and $p = tx + 2 \in \mathbb{Z}[t][x]$. Then p is not strongly primitive, since $\langle t, 2\rangle \ne \langle 1\rangle_R$. Meanwhile, the polynomial p is weakly primitive in $R[x]$. Indeed, if $t \mid 2\beta$ holds, then $t \mid \beta$ must hold too. Finally, we observe that weak primitivity is not invariant under a permutation of the coefficients. More precisely, and as a counter-example, consider $R = \mathbb{Z}_4[t]$, $p = \bar{2}x + t$ and $q = tx + \bar{2}$, the reciprocal of p. Then p is weakly primitive in $R[x]$, while q is not. Proposition 2 shows that the notion of weak primitivity is a generalization of the ordinary notion of primitivity over a unique factorization domain (UFD).

Proposition 2. *Let R be a UFD and $p = \sum_{i=0}^{e} a_i x^i \in R[x]$ with $a_e \ne 0$ and $e \ge 1$. Then, the following statements are equivalent*

(i) *p is weakly primitive in $R[x]$.*
(ii) $\operatorname{content}(p) := \gcd(a_0, \ldots, a_e) = 1$.

Proof. We prove (i) $\Rightarrow$ (ii). Assume that $\gcd(a_0, \ldots, a_e) \neq 1$. Then there is a prime factor f of $\gcd(a_0, \ldots, a_e)$. Let $\beta = a_e/f$. Then $a_e \mid \beta a_i$, for $0 \leq i \leq e-1$. Since $a_e \nmid \beta$, p is not weakly primitive, a contradiction.

We prove (ii) $\Rightarrow$ (i). Assume that there exists $\beta \in R$ such that

$$(\forall\, 0 \leq j \leq e-1)\ a_e \mid \beta a_j \quad \text{and} \quad a_e \nmid \beta.$$

Then $a_e \mid \text{content}(\beta p) = \beta\,\text{content}(p)$. Since $a_e \nmid \beta$, some prime factor f of a_e divides $\text{content}(p)$, a contradiction. □

The following property on weak primitivity will be used in the next section. It states the following fact: if one raises each coefficient of a weakly primitive polynomial p to some power, then the resulting polynomial is still weakly primitive. To avoid the cancelation of the leading coefficient of p, we assume that this coefficient is a regular element of the ground ring. The proof of Proposition 3 follows directly from Lemmas 2 and 3.

Proposition 3. *Let $p = \sum_{i=0}^{e} a_i x^i \in R[x]$ with a_e being regular in R, and $\{n_i \mid 0 \leq i \leq e\}$ be a set of non-negative integers. Define $q = \sum_{i=0}^{e} a_i^{n_i} x^i$. If p is weakly primitive, then q is also weakly primitive.*

Lemma 2. *Let $p = a_0 + \cdots + a_e x^e \in R[x]$ with a_e being regular in R and n be a non-negative integer. If p is weakly primitive, then $p_n = a_0 + \cdots + a_{e-1}x^{e-1} + a_e^n x^e$ is also weakly primitive.*

Proof. By induction on $n \geq 0$. The case $n = 0$ follows from Remark 1. So we assume that the claim is true for $n-1$, that is, p_{n-1} is weakly primitive, with $n \geq 1$. Let $\beta \in R$ such that $a_e^n \mid a_i\beta$, for $0 \leq i \leq e-1$. There exist $h_0, \ldots, h_{e-1} \in R$ such that we have

$$a_e^n h_i = a_i \beta, \quad 0 \leq i \leq e-1. \tag{6}$$

Since p_{n-1} is weakly primitive and since we have $a_e^{n-1} \mid a_i\beta$, we deduce $a_e^{n-1} \mid \beta$, that is, there exists $h' \in R$ such that

$$a_e^{n-1} h' = \beta. \tag{7}$$

With (6) and (7) we have $a_e^n h_i = a_i a_e^{n-1} h'$, and then $a_e h_i = a_i h'$, since a_e is regular. Hence $a_e \mid a_i h'$. Since p is weakly primitive, $a_e \mid h'$ holds and there exists $h'' \in R$ such that

$$a_e h'' = h'. \tag{8}$$

By (7) and (8) we have $a_e^n h'' = \beta$. So $a_e^n \mid \beta$ and p_n is weakly primitive. □

Lemma 3. *Let $p = a_0 + \cdots + a_e x^e \in R[x]$ with $a_e \neq 0$ and n be a non-negative integer. Let j be an index such that $0 \leq j \leq e-1$. Define $q = a_0 + \cdots + a_j^n x^j + \cdots + a_e x^e = p + (a_j^n - a_j)x^j$. If p is weakly primitive, then q is also weakly primitive.*

Proof. The claim is clear if $n = 0$, so we assume that $n \geq 1$. Let $\beta \in R$ such that, for $0 \leq i \leq e-1$ and $i \neq j$

$$a_e \mid a_i\beta, \quad \text{and} \quad a_e \mid a_j^n \beta. \tag{9}$$

We prove that $a_e \mid \beta$ holds. We have, for $0 \leq i \leq e-1$ and $i \neq j$

$$a_e \mid a_i(a_j^{n-1}\beta), \quad \text{and} \quad a_e \mid a_j(a_j^{n-1}\beta).$$

Define $\beta' = a_j^{n-1}\beta$. Hence $a_e \mid \beta'$ holds, since p is weakly primitive. With (9), for $0 \leq i \leq e-1$ and $i \neq j$ we have

$$a_e \mid a_i\beta, \quad \text{and} \quad a_e \mid a_j^{n-1}\beta. \tag{10}$$

We deduce that $a_e \mid a_j^{n-2}\beta$ holds. Continuing in this manner, we reach $a_e \mid \beta$. Thus q is also weakly primitive. □

4. Primitive regular chain

In this section, we generalize the notion of primitivity to any regular chain T. Then we prove that $\text{sat}(T) = \langle T \rangle$ holds if and only if T is primitive.

Definition 2. Let $T = \{p_1, \ldots, p_m\} \subset \mathbf{k}[\boldsymbol{x}] = \mathbf{k}[x_1, \ldots, x_n]$ be a regular chain with $\mathrm{mvar}(p_1) \prec \cdots \prec \mathrm{mvar}(p_m)$. We say that T is *primitive* if for all $1 \leq k \leq m$, p_k is weakly primitive in $R[x_j]$ where $x_j = \mathrm{mvar}(p_k)$ and

$$R = \mathbf{k}[x_1, \ldots, x_{j-1}]/\langle p_1, \ldots, p_{k-1}\rangle.$$

Proposition 4 (*Base Case of Theorem 3*). *Let $p = a_e x^e + \cdots + a_0 \in \mathbf{k}[\boldsymbol{y}][x]$ and $c = \gcd_{\mathbf{k}[\boldsymbol{y}]}(a_0, \ldots, a_e)$, where $e \geq 1$ and $\boldsymbol{y}$ is a finite set of variables. Then we have $\langle p\rangle = \langle p\rangle : a_e^\infty \iff c = 1$.*

Proof. First, we prove that $\langle p\rangle \subsetneq \mathrm{sat}(p) := \langle p\rangle : a_e^\infty$ if $c \neq 1$. Denote $\bar{p} = p/c$. Then $a_e\bar{p} = a_e p/c \in \langle p\rangle$, hence $\bar{p} \in \mathrm{sat}(p)$. Assume that $\bar{p}$ is in $\langle p\rangle$. Then there exists $q \in \mathbf{k}[\boldsymbol{y}][x]$ such that $p/c = \bar{p} = pq$. It follows that $qc = 1$ which is a contradiction since $c \notin \mathbf{k}$. Therefore $\bar{p}$ is in $\mathrm{sat}(p)$ but not in $\langle p\rangle$.

Conversely, we prove that if $c = 1$ then $\mathrm{sat}(p) \subseteq \langle p\rangle$. For any $q \in \mathrm{sat}(p)$, there exist $n \in \mathbb{Z}_{\geq 0}$ and $\beta \in \mathbf{k}[\boldsymbol{y}][x]$ such that $a_e^n q = \beta p$. Taking the content w.r.t. x, we have

$$\begin{aligned} a_e^n \mathrm{content}(q, x) &= \mathrm{content}(\beta, x)\,\mathrm{content}(p, x) \\ &= \mathrm{content}(\beta, x). \end{aligned}$$

Thus $a_e^n \mid \beta$. There exists $\beta' \in \mathbf{k}[\boldsymbol{y}][x]$ such that $\beta = a_e^n \beta'$. So we have $a_e^n q = \beta p = a_e^n \beta' p$, and then $q = \beta' p$, that is, $q \in \langle p\rangle$. □

Remark 2. Let $T = \{p_1\}$ be a regular chain consisting of a single polynomial. By definition, T is primitive if and only if p_1 is weakly primitive in $R = \mathbf{k}[x_1, \ldots, x_{j-1}]$, where $x_j = \mathrm{mvar}(p_1)$. Since R is a UFD, it follows from Proposition 2, that T is primitive if and only if p_1 is primitive in ordinary sense, that is, whenever the gcd of the coefficients of p_1 (as a univariate polynomial in $R[x_j]$) is 1. Therefore, the notion of primitivity for a regular chain extends that of primitivity for a polynomial.

Theorem 3. *Let $T \subset \mathbf{k}[x_1, \ldots, x_n]$ be a regular chain. Then T is primitive if and only if $\langle T\rangle = \mathrm{sat}(T)$.*

Proof. We prove the theorem by induction on the number of polynomials in T. The base case is Proposition 4, where $|T| = 1$. Now assume that $T = \{p_1, \ldots, p_m\}$ consists of $m \geq 2$ polynomials with $\mathrm{mvar}(p_1) \prec \cdots \prec \mathrm{mvar}(p_m)$. We denote by T_k the regular chain consisting of the first k polynomials in T.

First, assume indirectly that T is not primitive. We need to prove that $\langle T\rangle$ is a proper subset of $\mathrm{sat}(T)$. Let k be the smallest integer such that p_k is not weakly primitive in $R[y]$, where $y = x_j = \mathrm{mvar}(p_k)$ and $R = \mathbf{k}[x_1, \ldots, x_{j-1}]/\langle T_{k-1}\rangle$. By Proposition 4, we know $k \geq 2$.

Let $p_k = a_e y^e + \cdots + a_0$. By induction, $\mathrm{sat}(T_{k-1}) = \langle T_{k-1}\rangle$ holds and thus a_e is regular in R. Since p_k is not weakly primitive over R, there exists $\beta \in \mathbf{k}[x_1, \ldots, x_{j-1}]$ such that, in R, we have

$$(\forall 0 \leq r \leq e-1)\ a_e \mid \beta a_r \quad \text{and} \quad a_e \nmid \beta.$$

Define $q_k = \beta p_k / a_e$. Then $q_k \in R[y]$, since

$$\frac{\beta}{a_e} p_k = \beta y^e + \sum_{0 \leq r < e} \frac{\beta a_r}{a_e} y^r.$$

We claim that $q_k \in \langle p_k\rangle : a_e^\infty$ and $q_k \notin \langle p_k\rangle$ in $R[y]$, which leads to $\mathrm{sat}(T_k) \neq \langle T_k\rangle$.

Indeed, we have $a_e q_k = \beta p_k \in \langle p_k\rangle$ in $R[y]$. Thus, $q_k \in \langle p_k\rangle : a_e^\infty$. Now if $q_k \in \langle p_k\rangle$, there exists $\alpha \in R[y]$ such that $q_k = \alpha p_k$ in $R[y]$. By the construction of q_k, $\deg(q_k, y)$ equals $\deg(p_k, y)$. Hence $\alpha \in R$ and $\beta - \alpha a_e = 0$ in R. This contradicts $a_e \nmid \beta$.

Second, we assume that T is primitive and show $\langle T\rangle = \mathrm{sat}(T)$. By induction, $\mathrm{sat}(T_{k-1}) = \langle T_{k-1}\rangle$ holds. We shall prove that $\mathrm{sat}(T_k) = \langle T_k\rangle$ holds, too. To do so, we consider $p \in \mathrm{sat}(T_k)$ and show that we have $p \in \langle T_k\rangle$. Let $\mathrm{mvar}(p) = x_i$ and $\mathrm{mvar}(p_k) = x_j$. If $i > j$, then $p \in \mathrm{sat}(T_k)$ if and only if all coefficients of p w.r.t x_i are in $\mathrm{sat}(T_k)$, since T_k is a regular chain. So we can concentrate on the case $p \in \mathbf{k}[x_1, \ldots, x_j]$.

Let h_{p_k} be the leading coefficient of p_k w.r.t. $y = x_j$, that is, w.r.t. the main variable of p_k. By virtue of Theorem 2, we have

$$\begin{aligned} \mathrm{sat}(T_k) &= \langle \mathrm{sat}(T_{k-1}), p_k\rangle : h_{p_k}^\infty \\ &= \langle \langle T_{k-1}\rangle, p_k\rangle : h_{p_k}^\infty. \end{aligned}$$

By virtue of Theorem 1, we have $\mathrm{prem}(p, T_k) = 0$, since $p \in \mathrm{sat}(T_k)$. Consequently, $\mathrm{prem}(p, p_k)$ is in $\mathrm{sat}(T_{k-1}) = \langle T_{k-1}\rangle$. Now the pseudo-division formula leads to

$$h_{p_k}^{\alpha} p = \mathrm{pquo}(p, p_k) p_k + \mathrm{prem}(p, p_k), \tag{11}$$

where $\alpha = \max\{0,\ \deg(p,\ y) - \deg(p_k,\ y) + 1\}$. If $\deg(p,\ y) < \deg(p_k,\ y)$, then $p = \mathrm{prem}(p, p_k) \in \langle T_{k-1}\rangle \subset \langle T_k\rangle$ holds and we are done. From now on, we assume that $\deg(p,\ y) \geq \deg(p_k,\ y)$ and we write $\alpha = \deg(p,\ y) - \deg(p_k,\ y) + 1$. With (11) we observe that we have the following equation in $R[y]$

$$h_{p_k}^{\alpha} p = q p_k. \tag{12}$$

We consider a more general situation: let $s \in \mathrm{sat}(T_k)$, let δ be a non-negative integer and let $u \in \mathbf{k}[x_1, \ldots, x_n]$ such that

$$h_{p_k}^{\delta} s = u\, p_k \tag{13}$$

holds in $R[y]$. In order to prove that $p \in \langle T_k\rangle$ holds, we prove that $s \in \langle T_k\rangle$ by induction on the number of terms in u. For simplicity, we denote

$$p_k = \sum_{i=0}^{e} a_i y^i \quad \text{and} \quad u = \sum_{i=0}^{f} b_i y^i,$$

with $a_e \neq 0$ and $b_f \neq 0$. Note that $a_e = h_{p_k}$.

If $u = 0$ in $R[y]$, then ${a_e}^{\delta} s = 0$ in $R[y]$. Since a_e is regular in R, we deduce $s = 0$ in $R[y]$, that is, $s \in \langle T_{k-1}\rangle$ and thus $s \in \langle T_k\rangle$. Assume that $u \neq 0$ in $R[y]$. Let f' be the largest integer such that $b_{f'} \notin \langle T_{k-1}\rangle$ and write $u' = \sum_{i=0}^{f'} b_i y^i$. We have

$$a_e^{\delta} s = u' p_k \quad \text{in } R[y]. \tag{14}$$

By Lemma 1, for any $0 \leq i \leq e$, we have $a_e^{\delta} \mid b_{f'} a_i^{f'+1}$ in R. Since p_k is weakly primitive in $R[y]$, by Proposition 3 we have $a_e^{\delta} \mid b_{f'}$ in R. Thus there exists $\gamma \in \mathbf{k}[x_1, \ldots, x_{j-1}]$, $\gamma \neq 0$ in R, such that we have $a_e^{\delta}\gamma = b_{f'}$ in R. We define

$$s' = s - \gamma y^{f'} p_k. \tag{15}$$

Since $s \in \mathrm{sat}(T_k)$ we have $s' \in \mathrm{sat}(T_k)$. Moreover we have

$$u' = a_e^{\delta}\gamma y^{f'} + \mathrm{tail}(u').$$

Therefore, the following holds in $R[y]$:

$$a_e^{\delta} s' = \mathrm{tail}(u') p_k. \tag{16}$$

By induction hypothesis, we have $s' \in \langle T_k\rangle$. With (15), we conclude $s \in \langle T_k\rangle$. □

5. Weak primitivity test

In this section, we point out the componentwise nature of weak primitivity. That is, if R can be written as a direct product of rings, then checking weak primitivity over R reduces to checking weak primitivity over each of its "components". We start with a straightforward lemma, whose proof is omitted.

Lemma 4. *Let $R_1, \ldots, R_n$ be commutative rings with 1. Let $R = \prod_{i=1}^{n} R_i$ be their direct product and let π_k be the canonical projection from R to R_k. Let $a, b \in R$. Then $a \mid b$ in R if and only if $\pi_k(a) \mid \pi_k(b)$ for each $1 \leq k \leq n$.*

Proposition 5. *Let $R = \prod_{i=1}^{n} R_i$ be a direct product of rings and let π_k be the canonical projection from R to R_k and τ_k be the canonical injection from R_k to R. Let $p = \sum_{i=0}^{e} a_i x^i \in R[x]$ be a polynomial with a_e regular in R. Then p is weakly primitive in $R[x]$ if and only if $\pi_k(p) = \sum_{i=1}^{e} \pi_k(a_i) x^i$ is weakly primitive in $R_k[x]$ for each $1 \leq k \leq n$.*

Proof. For any $1 \leq k \leq n$, denote $p_k = \pi_k(p)$. Since a_e is regular in R, $\pi_k(a_e) \neq 0$ for each k, and then each p_k is a polynomial of degree e.

First, we prove that if all p_k are weakly primitive then p is also weakly primitive. Let $\beta \in R$ satisfying $a_e \mid a_i\beta$ for $0 \le i \le e-1$. We need to prove that $a_e \mid \beta$ in R.

Applying π_k to $a_e \mid a_i\beta$, we have $\pi_k(a_e) \mid \pi_k(a_i)\pi_k(\beta)$, for $0 \le i \le e-1$. By the weak primitivity of p_k, we have $\pi_k(a_e) \mid \pi_k(\beta)$. So there exists $u_k \in R_k$ such that $\pi_k(a_e)u_k = \pi_k(\beta)$. Define $u = (u_1, \ldots, u_n) \in \prod_{i=1}^{n} R_i$. Then $\pi_k(u) = u_k$, and hence $\pi_k(a_e)\pi_k(u) = \pi_k(\beta)$, for each $1 \le k \le n$. By Lemma 4, $a_e \mid \beta$ in R. We proved that p is weakly primitive in $R[x]$.

Now we prove that, if p_k is not weakly primitive over R_k for *some* $1 \le k \le n$ then p is not weakly primitive over R. For simplicity, we assume that $k = 1$. So, there exists $\beta_1 \in R_1$ such that $\pi_1(a_e) \mid \pi_1(a_i)\beta_1$ for $0 \le i \le e-1$, but $\pi_1(a_e) \nmid \beta_1$. Define $\beta = \tau_1(\beta_1) = (\beta_1, 0, \ldots, 0) \in R$. Then we claim that $a_e \nmid \beta$ and $a_e \mid a_i\beta$ for $0 \le i \le e-1$. This implies that p is not weakly primitive over R, as desired.

Indeed, first we have $a_e \nmid \beta$, since $\pi_1(a_e) \nmid \pi_1(\beta) = \beta_1$. Second, to prove $a_e \mid a_i\beta$ for $0 \le i \le e-1$, by Lemma 4, we need to prove that $\pi_k(a_e) \mid \pi_k(a_i\beta)$ for $1 \le k \le n$ and $0 \le i \le e-1$. If $k = 1$, it follows from the choice of β_1. If $2 \le k \le n$, we have

$$\pi_k(a_i\beta) = \pi_k(a_i)\pi_k(\beta) = \pi_k(a_i) \cdot 0 = 0$$

for $1 \le i \le e-1$. Thus $\pi_k(a_e) \mid \pi_k(a_i\beta)$ holds for $1 \le i \le e-1$. □

Example 1. Let $T = \{p_1, p_2\}$ be a regular chain in $\mathbb{Q}[t \prec x \prec y]$ with $p_1 = x(x-t)$, $p_2 = (x+t)y + t$. Since $p_1 = x^2 - tx$ is strongly primitive in $(\mathbb{Q}[t])[x]$, p_1 is weakly primitive in $(\mathbb{Q}[t])[x]$. Let $R = \mathbb{Q}[t, x]/\langle x(x-t)\rangle$. Then we have

$$R = R_1 \times R_2 = \mathbb{Q}[x, t]/\langle x\rangle \times \mathbb{Q}[x, t]/\langle x - t\rangle \simeq \mathbb{Q}[t] \times \mathbb{Q}[t].$$

Over R_1, $p_2 = ty + t$ is not weakly primitive, since t is not invertible over R_1 and according to the definition we can choose $\beta = 1$. Hence T is not a primitive regular chain.

In order to generalize the construction of the above example into an algorithm, one would need to use algebraic factorization. In the next section, we propose a primitivity test for regular chains which avoids algebraic factorization, relying instead on polynomial GCDs modulo regular chains. Based on the algorithms and software tools available today, we view it as a practical solution, as confirmed in Section 8.

6. A primitivity test algorithm

In Section 4, we defined the notion of a primitive regular chain which generalizes that of a primitive polynomial over a UFD. In this section, we present another characterization on primitivity in terms of regularity of a polynomial. As a consequence, we obtain an algorithm to test whether a regular chain is primitive or not.

Lemmas 5–8 are well-known facts. The proofs of Lemmas 5 and 8 are straightforward. Lemma 6 can be found as Lemma 9.2.3 in Ischebeck and Rao (2005) whereas Lemma 7 is in Coquand et al. (2003, Lemma 7).

Lemma 5. *Let I be a proper ideal of R and let h be an element of R. Then h is regular modulo I if and only if $I = I : h^\infty$ holds.*

Lemma 6. *Let a and b be two regular elements of R. Assume that a and b are not invertible. If a is regular modulo $\langle b\rangle$, then b is also regular modulo $\langle a\rangle$.*

Lemma 7 (*McCoy Lemma*)**.** *A non-zero polynomial $f \in R[x]$ is a zerodivisor if and only if there exists a non-zero element $a \in R$ such that $af = 0$ holds.*

Lemma 8. *Let $f \in R[x]$ be a non-constant polynomial. If its leading coefficient is a regular element in R, then f is not a unit.*

Proposition 6. *Let R be a Noetherian commutative ring with* 1*. Consider a polynomial $f = \sum_{i=0}^{n} a_i x^i \in R[x]$. Assume that n is at least* 1 *and a_n is regular in R. Then $\langle f\rangle = \langle f\rangle : a_n^\infty$ holds if and only if a_n is invertible in R, or* tail(f) *is regular modulo $\langle a_n\rangle$.*

Proof. If a_n is invertible in R, then clearly $\langle f\rangle : a_n^\infty = \langle f\rangle$ holds. So we assume that a_n is not invertible in R. Note that both a_n and f are regular in $R[x]$; this follows from Lemma 7. Since a_n is not invertible in R, a_n is not invertible in $R[x]$ either. Since a_n is regular in R, it follows from Lemma 8 that f is not invertible in $R[x]$. Then, applying Lemmas 5 and 6, we deduce

$$\begin{aligned}\langle f\rangle = \langle f\rangle : {a_n}^\infty &\iff a_n \text{ is regular modulo } \langle f\rangle\\ &\iff f \text{ is regular modulo } \langle a_n\rangle\\ &\iff \mathrm{tail}(f) \text{ is regular modulo } \langle a_n\rangle.\end{aligned}$$

This completes the proof. □

The following corollary may be seen as another characterization of the primitivity of a regular chain. This also provides an algorithm for checking whether a regular chain is primitive or not.

Corollary 1 (*Primitivity Test of a Regular Chain*)**.** *Let $T \subset \mathbf{k}[x_1, \ldots, x_{s-1}]$ be a primitive regular chain. Let $p = \sum_{i=0}^{e} a_i x_s^i \in \mathbf{k}[x_1, \ldots, x_s]$ with a_e being regular modulo* $\mathrm{sat}(T)$*. Denote* $\mathrm{tail}(p) = \sum_{i=0}^{e-1} a_i x_s^i$*. Then $T \cup \{p\}$ is a primitive regular chain if and only if a_e is invertible modulo* $\mathrm{sat}(T)$*, or* $\mathrm{tail}(p)$ *is a regular polynomial modulo $\langle T \cup \{a_e\}\rangle$.*

Proof. This is a direct consequence of Proposition 6, Theorem 3 and the definition of a regular chain. □

Thus the problem of checking whether a regular chain $T \cup \{p\}$ is primitive or not, reduces to checking whether the polynomial $\mathrm{tail}(p)$ is regular or not modulo $\langle T, a_e\rangle$. We next show that (T, a_e) in Corollary 1 generates an unmixed ideal; this result is crucial in view of Algorithm 1 below. Indeed, it allows us to deal with the following subtle point: a polynomial p which is regular modulo the radical $\sqrt{I}$ of an ideal I, may not be regular modulo I. For example, consider $p = y$ and $I = \langle xy, x^2\rangle$. Then y is a zerodivisor modulo I but y is regular modulo $\sqrt{I} = \langle x\rangle$. If I is unmixed, then p is regular modulo I if and only if p is regular modulo $\sqrt{I}$.

Lemma 9. *Let $R = \mathbf{k}[x_1, \ldots, x_n]$ and T be a primitive regular chain of R. If $t \in R$ is regular but not invertible modulo* $\mathrm{sat}(T)$*, then (T, t) is a regular sequence of R and the ideal $\langle T, t\rangle$ is unmixed with dimension $n - |T| - 1$.*

Proof. Denote $T_i = T \cap \mathbf{k}[x_1, \ldots, x_i]$. Since T is primitive, $\mathrm{sat}(T_i) = \langle T_i\rangle$ holds for each i. Thus T is already a regular sequence of R. Now since t is regular but not invertible modulo $\mathrm{sat}(T) = \langle T\rangle$, by definition (T, t) is a regular sequence.

Let $I = \langle T, t\rangle$ and $d = |T|$. According to the Principal Ideal Theorem (see Eisenbud, 1994, Theorem 10.2), the dimension $\dim(I)$ of I is at least $n - (d + 1)$. On the other hand, since (T, t) is a regular sequence of length $d + 1$, the dimension of I is at most $n - (d + 1)$. Hence, $\dim(I) = n - (d + 1)$ and then I is unmixed, by the Macaulay Unmixedness Theorem (see Sturmfels, 2002, Theorem 5.7). □

Remark 3. Before proving the above algorithm, we comment on its subprocedures and possible optimization.

(1) The function **Triangularize** decomposes a polynomial system F into a finite set of regular chains U_i such that $\sqrt{\langle F\rangle} = \cap_i \sqrt{\mathrm{sat}(U_i)}$ holds; this is called a triangular decomposition of F in the sense of Kalkbrener (Aubry and Moreno Maza, 1999). According to the above specification, the set of the associated primes of $\sqrt{\langle F\rangle}$ are "implicitly" represented by U_i's . **Triangularize** is one of the core functions in the RegularChains library in Maple (Lemaire et al., 2005); it implements the triangular decomposition algorithm of Moreno Maza (1999). While computing in Kalkbrener's sense, it has the same specification as the function **solve**$_n$ in Kalkbrener (1993), although the algorithms of Moreno Maza (1999) and Kalkbrener (1993) are quite different. Apart from Kalkbrener's sense, **Triangularize** can also work in the Lazard sense (see Aubry and Moreno Maza, 1999), where all solutions of the input systems will be explicitly represented by means of regular chains. For input systems in positive dimension, this function runs faster in Kalkbrener's sense since only *generic* solutions are represented explicitly in this sense.

Algorithm 1 IsPrimitive

Input: T, a regular chain of $\mathbf{k}[x_1, \ldots, x_n]$.
Output: true if T is primitive, false otherwise.

```
1: if |T| = 1 then
2:   t ← the defining polynomial of T
3:   if content(t, mvar(t)) ∈ k then return true else return false
4: else
5:   write T as T' ∪ {t}, where t has the greatest main variable
6:   if not IsPrimitive(T') then
7:     return false
8:   else
9:     h ← init(t), r ← tail(t)
10:    for U ∈ Triangularize(T' ∪ {h}) do
11:      if ires(r, U) = 0 then return false
12:    end for
13:    return true
14:  end if
15: end if
```

(2) The use of **Triangularize** seems hard to avoid. The purpose is to represent all associated primes of the ideal $\langle T \cup \{h\}\rangle$ by means of regular chains. Geometrically, it is the intersection of the zero set of T with the hypersurface defined by h.
(3) Algorithm 1 is implemented in the RegularChains library. The code includes various optimizations. For instance, and as noted in Remark 1, if a coefficient a_i of $t = a_e x^e + \cdots + a_0$ is an invertible constant, then lines 10–12 can be skipped since t is strongly primitive.

Proof. We prove the above algorithm **IsPrimitive**. Its termination of the algorithm follows from the fact that in each recursive call the number of polynomials in the input regular chain decreases by 1. For the correctness, we proceed by induction on the number of polynomials in the regular chain T. When $|T| = 1$, the specification follows from Remark 2. So we assume that $|T| > 1$. Definition 2 and Theorem 3 imply that if T is primitive then T' is also primitive. So we assume that T' is primitive and branch to line 9. Let $\mathcal{U}$ be the output of **Triangularize** in line 10 and let $I = \langle T' \cup \{h\}\rangle$. From the specification of **Triangularize**, we have

$$\bigcap_{U \in \mathcal{U}} \sqrt{\mathrm{sat}(U)} = \sqrt{I}.$$

By Corollary 1, we need to distinguish two cases: h is invertible (resp. not invertible) modulo $\langle T'\rangle = \mathrm{sat}(T')$. If h is invertible modulo $\langle T'\rangle$ then $\mathcal{U}$ is empty, and the algorithm correctly returns true. Assume from now on that h is not invertible modulo $\langle T'\rangle$. In this case by Lemma 9, the triangular decomposition $\mathcal{U}$ is not empty. So T is primitive if and only if r is regular modulo I. By Lemma 9 again, the ideal I is unmixed and therefore T is primitive if and only if r is regular modulo $\sqrt{I}$. This holds if and only if r is regular modulo $\mathrm{sat}(U)$ for each $U \in \mathcal{U}$. Finally, the correctness of Algorithm 1 follows from Theorem 1. □

Example 2. Let $R = \mathbf{k}[z \prec y \prec x]$ be a polynomial ring and $T = \{t_1, t_2\}$ be a regular chain of R with $t_1 = y^5 - z^4$, $t_2 = zx - y^2$. Clearly, $\{t_1\}$ is a primitive regular chain. Let $I = \langle t_1, \mathrm{lc}(t_2)\rangle = \langle t_1, z\rangle = \langle z, y^5\rangle$. In Algorithm 1 the call to **Triangularize** will produce $\sqrt{I} = \sqrt{\mathrm{sat}(U)}$, where $U = \{z, y\}$ is a regular chain. Thus, the computation

$$\mathrm{ires}(\mathrm{tail}(t_2), U) = \mathrm{ires}(-y^2, U) = 0$$

implies that $\mathrm{tail}(t_2) = -y^2$ is not regular modulo I. Thus T is not primitive. In fact, the prime ideal $\mathrm{sat}(T) = \langle x^3 - yz, xz - y^2, z^2 - x^2y\rangle$ cannot be generated by only two polynomials (see Şahin, 2002, page 43). Hence, in *any* variable ordering, one cannot find a primitive regular chain C such that $\langle C\rangle = \mathrm{sat}(T)$.

7. An application to the inclusion test of saturated ideals

A fundamental problem in the theory of regular chains is the inclusion test for saturated ideals, that is, deciding whether $\mathrm{sat}(T) \subseteq \mathrm{sat}(U)$ holds for two regular chains T and U. For a regular chain T, denote by $\mathrm{mvar}(T)$ the set of the main variables of the polynomials in T, which is also called the set of algebraic variables of T. In this section, we first show that when T and U share the same set of algebraic variables, the inclusion test is simple. Then we point out that the notion of primitivity presented in this paper solves the inclusion test problem partially.

Lemma 10. *Let T and U be two regular chains. If $\mathrm{sat}(T) \subseteq \mathrm{sat}(U)$ and $|T| = |U|$ hold, then each associated prime of $\mathrm{sat}(U)$ is also an associated prime of $\mathrm{sat}(T)$.*

Proof. Let $\mathcal{T}$ and $\mathcal{U}$ be the set of associated primes of $\mathrm{sat}(T)$ and $\mathrm{sat}(U)$, respectively. Then we have

$$\sqrt{\mathrm{sat}(T)} = \bigcap_{P \in \mathcal{T}} P \quad \text{and} \quad \sqrt{\mathrm{sat}(U)} = \bigcap_{Q \in \mathcal{U}} Q.$$

Since $\mathrm{sat}(T) \subseteq \mathrm{sat}(U)$ implies $\sqrt{\mathrm{sat}(T)} \subseteq \sqrt{\mathrm{sat}(U)}$, for each $Q \in \mathcal{U}$ there exists $P \in \mathcal{T}$ such that $P \subseteq Q$. Since T and U are unmixed with same height, $\dim(P)$ equals $\dim(Q)$, which implies $Q = P$. Hence $\mathcal{U}$ is a subset of $\mathcal{T}$. □

Proposition 7. *Let T and U be two regular chains with the same set of algebraic variables. Write T as $T = T' \cup \{t\}$ with t having the largest main variable. Then $\mathrm{sat}(T) \subseteq \mathrm{sat}(U)$ if and only if $\mathrm{sat}(T') \subseteq \mathrm{sat}(U)$ and $\mathrm{prem}(t, U) = 0$.*

Proof. Clearly, we only need to show that $\mathrm{sat}(T) \subseteq \mathrm{sat}(U)$ holds if $\mathrm{sat}(T') \subseteq \mathrm{sat}(U)$ and $\mathrm{prem}(t, U) = 0$.

Denote by h the initial of t. We first prove that h is regular modulo $\mathrm{sat}(U)$. Since h is regular modulo $\mathrm{sat}(T')$, h is not contained in any associated prime of $\mathrm{sat}(T')$. Let u be the polynomial in U such that $\mathrm{mvar}(t) = \mathrm{mvar}(u)$ and define $U' = U \setminus \{u\}$. Then we have $\mathrm{sat}(T') \subseteq \mathrm{sat}(U')$. By Lemma 10, h is not contained in any associated prime of $\mathrm{sat}(U')$. Hence h is regular modulo $\mathrm{sat}(U')$. It follows that h is regular modulo $\mathrm{sat}(U)$, since the main variable of h is smaller than that of u.

For arbitrary $f \in \mathrm{sat}(T)$, we have $\mathrm{prem}(f, t) \in \mathrm{sat}(T') \subseteq \mathrm{sat}(U)$. By the pseudo-division formula, $h^e f = \mathrm{prem}(f, t) + q\,t$ for some $e \geq 0$ and some q. Since $\mathrm{prem}(t, U) = 0$, we have $t \in \mathrm{sat}(U)$. Therefore $h^e f$ belongs to $\mathrm{sat}(U)$, which implies $f \in \mathrm{sat}(U)$ since h is regular modulo $\mathrm{sat}(U)$. □

Example 3. Let $R = \mathbf{k}[x \prec y \prec z]$ and let $T = \{xz + y\}$ and $U = \{x, y\}$ be regular chains of R. Then $\mathrm{sat}(T) = \langle xz + y \rangle \subsetneq \langle x, y \rangle = \mathrm{sat}(U)$ holds, although we have $\mathrm{mvar}(T) = \{z\}$ and $\mathrm{mvar}(U) = \{x, y\}$.

In practice, the inclusion $\mathrm{sat}(T) \subseteq \mathrm{sat}(U)$ is often established by proving that $\langle T \rangle \subseteq \mathrm{sat}(U)$ holds and that all initials in T are regular modulo $\mathrm{sat}(U)$. This simple criterion follows immediately from the definition of a saturated ideal and Lemma 5.

Now with the notion of primitivity for a regular chain, we have another useful way to detect whether $\mathrm{sat}(T) \subseteq \mathrm{sat}(U)$ holds. That is, $\mathrm{sat}(T) \subseteq \mathrm{sat}(U)$ holds whenever $\langle T \rangle \subseteq \mathrm{sat}(U)$ holds and T is primitive. In the above example, the initial of $zx + y$ is not regular modulo $\mathrm{sat}(U)$. However, we know that $\mathrm{sat}(T)$ is contained in $\mathrm{sat}(U)$, since T is primitive and $\langle T \rangle \subseteq \mathrm{sat}(U)$ holds. In Section 8, we shall see that the algorithm **IsPrimitive** is efficient and primitive regular chains appear quite often in practice.

Corollary 2 below is a direct consequence of Proposition 7, which shows that it is an easy task to check whether two regular chains have the same saturated ideal. Actually, testing $\mathrm{sat}(T) = \mathrm{sat}(U)$ can be done "directly" without testing the inclusions $\mathrm{sat}(T) \subseteq \mathrm{sat}(U)$ and $\mathrm{sat}(U) \subseteq \mathrm{sat}(T)$. The algorithm concluding this section combines together the different criteria reported above for testing the inclusion of saturated ideals. Observe that this algorithm is not always able to decide whether the inclusion holds or not.

Corollary 2. *Let $T = T \cup \{t\}$ and $U = U' \cup \{u\}$ be two regular chains with t and u having the greatest main variable in T and U, respectively. The equality $\mathrm{sat}(T) = \mathrm{sat}(U)$ holds if and only if the following conditions hold*

(1) $\mathrm{sat}(T') = \mathrm{sat}(U')$,
(2) $\mathrm{mvar}(t) = \mathrm{mvar}(u)$,
(3) $t \in \mathrm{sat}(U)$ *and* $u \in \mathrm{sat}(T)$.

Algorithm 2 IsIncluded

Input: T and U, regular chains of $\mathbf{k}[x_1, \ldots, x_n]$.
Output: If true (resp. false) is returned then $\mathrm{sat}(T) \subseteq \mathrm{sat}(U)$ holds (resp. does not hold). If failed is returned then the inclusion could not be proved nor disproved.

if $T = \emptyset$ **then return** true **end if**
if $U = \emptyset$ **then return** false **end if**
if $\mathrm{mvar}(T) = \mathrm{mvar}(U)$ **then**
  $v := \max \mathrm{mvar}(T)$
  $T' := T \setminus \{T_v\}$
  if IsIncluded(T', U) **and** $\mathrm{prem}(T_v, U) = 0$ **then return** true **end if**
end if
if $T \subseteq \mathrm{sat}(U)$ **then**
  if $\mathrm{ires}(\prod_{t \in T} \mathrm{init}(t), U) \neq 0$ **then return** true **end if**
  if IsPrimitive(T) **then return** true **end if**
end if
return failed

8. Experimentation

We have implemented the algorithm **IsPrimitive** on top of the RegularChains library in Maple (Lemaire et al., 2005). The experimentation, described hereafter, was conducted on well-known problems used in Chen et al. (2007) and the tests were performed in Maple 11 on an Intel Pentium 4 machine (3.20GHz CPU, 2.0GB memory).

First, we computed their triangular decompositions using the **Triangularize** command in the sense of Kalkbrener. Then, we applied the **IsPrimitive** algorithm to each regular chain in the output.

In Table 1, we summarize the features of the problems and our experimental results. The names of the problems are listed in the first column. The second column gives the number n of variables and the maximal total degree d. For each triangular decomposition (which is a list of regular chains), we record the total running time (in seconds) of **IsPrimitive** in the third column. The last column is the result of mapping **IsPrimitive** to each triangular decomposition: in each of these patterns Y stands for *true* and N for *false*.

These data show that the procedure **IsPrimitive** is efficient in practice. This agrees with the fact that, in Algorithm 1, the input polynomial set in each call to **Triangularize** is rather structured. We also observe that primitive regular chains appear quite often in the output of triangular decompositions.

9. Discussion

We have generalized the notion of primitivity from univariate polynomials to regular chains. This has allowed us to establish a necessary and sufficient condition for a regular chain T to generate its saturated ideal $\mathrm{sat}(T)$. Assume that T is not empty and write $T = T' \cup \{p\}$ where p is the polynomial of T with the largest main variable. Theorem 3 states that the equality $\langle T \rangle = \mathrm{sat}(T)$ holds whenever $\langle T' \rangle = \mathrm{sat}(T')$ holds and the polynomial p is *weakly primitive* over $\mathbf{k}[\boldsymbol{x}]/\langle T' \rangle$. This latter property is a generalization of the usual notion of primitivity for polynomials over a UFD.

Examining the proof of Theorem 3, we make the following observation. When p is not weakly primitive over $\mathbf{k}[\boldsymbol{x}]/\langle T' \rangle$, the proof exhibits a polynomial q which belongs to $\mathrm{sat}(T)$ but not to $\langle T \rangle$. When p is weakly primitive over $\mathbf{k}[\boldsymbol{x}]/\langle T' \rangle$, the proof shows that every polynomial q of $\mathrm{sat}(T)$ belongs to $\langle T \rangle$. The argument is constructive providing that one has at hand an algorithm for dividing a by b modulo $\langle T' \rangle$, where b is a polynomial regular modulo $\langle T' \rangle$ and is a multiple of the polynomial a modulo $\langle T' \rangle$. This can be done via Gröbner basis computations (see Monagan and Pearce, 2006). An algorithmic solution based on the algorithms of the RegularChains library is an ongoing research work.

Table 1
Tests for **IsPrimitive** on 14 examples.

System	(n, d)	Time	Pattern
KdV575	(26, 3)	3.525	[Y, Y, Y, Y, Y, Y, Y]
MontesS11	(6, 4)	.001	[Y]
MontesS16	(15, 2)	.103	[Y, Y, Y, N, Y, Y, Y]
Wu-Wang2	(13, 3)	0.099	[Y, N, Y, Y, Y]
MontesS10	(7, 3)	.145	[N]
Lazard2001	(7, 4)	2.314	[Y, Y, Y, N, Y, N]
Lanconelli	(11, 3)	.062	[N, Y]
Wang93	(5, 3)	.142	[N]
Leykin-1	(8, 4)	.228	[Y, Y, Y, Y, Y, Y, Y, Y, N, Y, Y, Y, N, N]
MontesS14	(5, 4)	1.171	[Y, N, N]
MontesS15	(12, 2)	.312	[N]
Maclane	(10, 2)	.157	[Y, Y, N, Y, N]
MontesS12	(8, 2)	.042	[N]
Liu-Lorenz	(5, 2)	1.117	[N, Y]

Theorem 3 and its proof do not lead directly to an algorithm for testing the equality $\langle T \rangle = \mathrm{sat}(T)$. Algorithm 1 provides such a decision procedure. This algorithm reduces to testing whether a polynomial is regular modulo an ideal. Fortunately the involved ideal is unmixed which allows us to rely on the algorithms of the RegularChains library avoiding Gröbner basis computations. Our experimentation illustrates the practical efficiency of Algorithm 1.

Algorithm 1 does not generalize easily in the differential setting. Indeed, consider the polynomial $p = u_x^2 - 4u$ as in (Ritt, 1950, example 1 page 120). We recall hereafter that we have $[u_x^2 - 4u] \subsetneq [u_x^2 - 4u] : \{u_x\}^\infty$. This indicates that even in the case of a single polynomial, the problem is much harder in the differential setting since the case of a single polynomial in the algebraic setting is obvious (line 3 of Algorithm 1). It is obvious to show that $u_{xx} - 2 \in [u_x^2 - 4u] : \{u_x\}^\infty$ since $dp/dx = 2u_x(u_{xx} - 2)$. However $u_{xx} - 2 \notin [u_x^2 - 4u]$ holds for the following reason: the solution $u = 0$ for $[u_x^2 - 4u]$ does not cancel $u_{xx} - 2$ which implies: $u_{xx} - 2 \notin [u_x^2 - 4u]$. Thus, we have $[u_x^2 - 4u] \subsetneq [u_x^2 - 4u] : \{u_x\}^\infty$.

References

Arnold, J., Gilmer, R., 1970. On the contents of polynomials. Proc. Amer. Math. Soc. 24, 556–562.
Aubry, P., Lazard, D., Moreno Maza, M., 1999. On the theories of triangular sets. J. Symbolic. Comput. 28 (1–2), 105–124.
Aubry, P., Moreno Maza, M., 1999. Triangular sets for solving polynomial systems: a comparative implementation of four methods. J. Symbolic. Comp. 28 (1–2), 125–154.
Boulier, F., Lemaire, F., Moreno Maza, M., 2006. Well known theorems on triangular systems and the D5 Principle, In: Transgressive Computing 2006, Universidad de Granada.
Chen, C., Lemaire, F., Golubitsky, O., Moreno Maza, M., Pan, W., 2007. Comprehensive triangular decomposition. In: Proc. of CASC 2007. In: Lecture Notes in Computer Science, vol. 4770. Springer-Verlag, pp. 73–101.
Chen, C., Lemaire, F., Moreno Maza, M., Pan, W., Xie, Y., 2007. Efficient computations of irredundant triangular decompositions with the RegularChains library. In: Proc. of CASA2007. In: Lecture Notes in Computer Science, vol. 4488. Springer-Verlag, pp. 268–271.
Chou, S.C., Gao, X.S., 1991. On the dimension of an arbitrary ascending chain. Chinese Bull. Sci. 38, 799–804.
Coquand, T., Ducos, L., Lombardi, H., Quitté, C., 2003. L'idéal des coefficients du produit de deux polynômes. Rev. Math. l'enseign. Supér. 113 (3), 25–39.
Corso, A., Vasconcelos, W.V., Villarreal, R.H., 1998. On the contents of polynomials. J. Pure. Appl. Algebra 125 (1–3), 117–127.
Eisenbud, D., 1994. Commutative Algebra. Springer-Verlag.
Hubert, E., 2001. Notes on triangular sets and triangulation-decomposition algorithms I: Polynomial systems. In: SNSC, pp. 1–39.
Ischebeck, F., Rao, R.A., 2005. Ideals and Reality, Projective Modules and Number of Generators of Ideals. Springer-Verlag.
Kalkbrener, M., 1993. A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. J. Symb. Comp. 15, 143–167.
Kalkbrener, M., 1998. Algorithmic properties of polynomial rings. J. Symbolic. Comput. 26 (5), 525–581.
Lemaire, F., Moreno Maza, M., Xie, Y., 2005. The RegularChains library in Maple 10. In: Ilias S. Kotsireas, (Ed.), Maple Conference 2005, pp. 355–368.
Lemaire, F., Moreno Maza, M., Pan, W., Xie, Y., 2008. When does (T) equal Sat(T)? In: Proc. ISSAC'08. ACM Press, pp. 207–214.
Monagan, M., Pearce, R., 2006. Rational simplification modulo a polynomial ideal. In: ISSAC'06. ACM, pp. 239–245.
Moreno Maza, M., 1999. On triangular decompositions of algebraic varieties. Technical Report TR 4/99. NAG Ltd., Oxford, UK, Presented at the MEGA-2000 Conference, Bath, England. http://www.csd.uwo.ca/~moreno.
Moreno Maza, M., Rioboo, R., 1995. Polynomial gcd computations over towers of algebraic extensions. In: Proc. AAECC-11. In: Lecture Notes in Computer Science, vol. 948. Springer, pp. 365–382.

Ritt, Joseph Fels, 1950. Differential Algebra. Dover Publications Inc., New York, Available at http://www.ams.org/online_bks/coll33.
Şahin, M., 2002. On the minimal number of elements generating an algebraic set. Master thesis, Bilkent University.
Sturmfels, B., 2002. Solving Systems of Polynomial Equations. Amer. Math. Soc.
Wang, D., 2000. Computing triangular systems and regular systems. J. Symbolic. Comput. 30 (2), 221–236.
Wu, W.T., 1986. On zeros of algebraic equations — an application of Ritt principle. Kexue Tongbao 31 (1), 1–5.
Yang, L., Zhang, J., 1991. Searching dependency between algebraic equations: an algorithm applied to automated reasoning. Technical Report IC/91/6, International Atomic Engery Angency, Miramare, Trieste, Italy.